CLAIMS

WE CLAIM:

1. A distributed firewall (DFW) for use on an end system, comprising:

an authentication component for providing user authentication for connection attempts from users attempting to access the end system via a network;

an access control component for providing purpose authorization for authenticated users based on rules in a connection policy associating users with purposes;

an enforcement component for enforcing the connection policy rule for the authenticated user from whom the traffic is sent as the traffic is received; and

wherein the authentication component utilizes an aggregate of the users in the connection policy to authenticate users.

2. The DFW of claim 1, wherein the authentication component utilizes Internet key exchange (IKE) protocol to authenticate users in IKE main mode (MM) based on the aggregate of users in the connection policy.

3. The DFW of claim 2, wherein the authentication component utilizes the rule in the connection policy associated with the authenticated user in IKE quick mode (QM) to complete the authentication.

4. The DFW of claim 3, wherein the authentication component transmits a secure notify message to the authenticated user when the authenticated user sends traffic in QM

that exceeds an authority governed by the rule in the connection policy associated with the authenticated user.

5. The DFW of claim 3, wherein the enforcement component utilizes Internet protocol security (IPSec) protocol to maintain security of communications from the authenticated user when the communications are within the rule in the connection policy.

6. The DFW of claim 5, wherein the enforcement component enables IPSec on a socket for communications from the authenticated user and binds the socket in exclusive mode so that the context of the binder of the socket is preserved.

7. The DFW of claim 1, further comprising an inspection component for inspecting packets from an authenticated user.

8. The DFW of claim 1, wherein the connection policy is defined in a pluggable policy component.

9. The DFW of claim 8, wherein the pluggable policy component is downloaded from a centralized administrative policy.

10. The DFW of claim 8, wherein the pluggable policy component is modifiable on the end system.

11. The DFW of claim 10, further comprising an access control component through which the connection policy may be defined.

12. The DFW of claim 1, further comprising an access control component having a user interface (UI) through which the connection policy is defined.

13. A method of providing user authentication/authorization in a distributed firewall on an end system, comprising the steps of:

receiving a connection request from a user;

performing main mode (MM) authentication of the connection request via Internet key exchange (IKE) protocol based on an aggregate of users listed in a connection policy;

receiving communications from the user;

performing quick mode (QM) authentication of the communications via IKE based on a rule for the user in the connection policy;

completing the QM authentication when the communications are within a scope of the rule for the user in the connection policy; and

enforcing the rule for the user for subsequent communication when the QM completes.

14. The method of claim 13, wherein the step of performing MM authentication comprises the steps of:

checking a certificate of the connection request against an aggregate listing of all authorized users in the connection policy; and

completing MM authentication when the certificate matches an entry in the aggregate listing.

15. The method of claim 13, further comprising the step of transmitting a secure notify message to the user when the communications attempt to exceed the rule for the user in the connection policy.

16. The method of claim 13, wherein the step of enforcing the rule for the user for subsequent communication comprises the steps of enabling IPSec on a socket for the communication, and forcing the socket to be bound in exclusive mode.

17. The method of claim 13, wherein the end system has multiple accounts thereon, wherein the step of receiving a connection request from a user includes the step of receiving a connection request having an account ID hint included therewith, and wherein the step of performing main mode (MM) authentication of the connection request via Internet key exchange (IKE) protocol includes the step of performing MM authentication of the connection request via IKE based on an aggregate of users listed in a connection policy for one of the accounts identified by the account ID hint.

18. The method of claim 17, wherein the step of performing quick mode (QM) authentication of the communications via IKE based on a rule for the user in the connection policy comprises the step of performing QM authentication based on a rule

for the user in the connection policy for one of the accounts identified by the account ID hint.

19. The method of claim 13, further comprising the step of downloading the connection policy from a central administration.

20. The method of claim 13, further comprising the steps of displaying an access control user interface, receiving input from a user of the end system, using the input to define the rules of the connection policy.

21. In a computer system having a graphical user interface including a display and a user interface selection device, a method of displaying and selecting a connection policy on the display comprises the steps of:

retrieving a set of applications processes to which access controls may be defined;

retrieving a listing of authorized users;

displaying the set of applications in association with users who are authorized to access each application defined in the connection policy;

receiving a user input signal indicating a desired modification to the displayed associations and thereafter modifying the connection policy in accordance with the user input; and

displaying the set of applications in association with a modified list of users who are authorized to access each application defined in the modified connection policy.

22. The method of claim 21, wherein the step of receiving a user input indicating a desired modification to the displayed associations comprises the step of receiving a user input indicating a desired addition of a user for a selected application process, further comprising the steps of displaying a list of all authorized users, receiving an authorized user selection input to add a new authorized user association to the selected application process.

23. The method of claim 21, wherein the step of receiving a user input indicating a desired modification to the displayed associations comprises the step of receiving a user input indicating a desired removal of a user for a selected application process, further comprising the steps of displaying a list of all authorized users associated with the selected application process, receiving an authorized user deletion input to remove an authorized user association from the selected application process.

24. The method of claim 21, further comprising the steps of displaying a user selectable indicator to secure the computer system, receiving a user input selection of the user selectable indicator, and thereafter securing the computer system in accordance with the connection policy.

25. The method of claim 24, further comprising the steps of displaying a user selectable indicator indicating the that the computer system is secure, receiving a user input selection of the user selectable indicator, and thereafter un-securing the computer system.

26. A computer-readable medium having computer-executable instruction for performing the steps of receiving a connection request from a user, performing main mode (MM) authentication of the connection request via Internet key exchange (IKE) protocol based on an aggregate of users listed in a connection policy, receiving communications from the user, performing quick mode (QM) authentication of the communications via IKE based on a rule for the user in the connection policy, completing the QM authentication when the communications are within a scope of the rule for the user in the connection policy, and enforcing the rule for the user for subsequent communication when the QM completes.

27. The method of claim 26, wherein the step of performing MM authentication comprises the steps of checking a certificate of the connection request against an aggregate listing of all authorized users in the connection policy, and completing MM authentication when the certificate matches an entry in the aggregate listing.

28. The method of claim 26, further comprising the step of transmitting a secure notify message to the user when the communications attempt to exceed the rule for the user in the connection policy.

29. The method of claim 26, wherein the step of enforcing the rule for the user for subsequent communication comprises the steps of enabling IPSec on a socket for the communication, and forcing the socket to be bound in exclusive mode.

30. The method of claim 26, wherein the end system has multiple accounts thereon, wherein the step of receiving a connection request from a user includes the step of receiving a connection request having an account ID hint included therewith, and wherein the step of performing main mode (MM) authentication of the connection request via Internet key exchange (IKE) protocol includes the step of performing MM authentication of the connection request via IKE based on an aggregate of users listed in a connection policy for one of the accounts identified by the account ID hint.

31. The method of claim 30, wherein the step of performing quick mode (QM) authentication of the communications via IKE based on a rule for the user in the connection policy comprises the step of performing QM authentication based on a rule for the user in the connection policy for one of the accounts identified by the account ID hint.

32. The method of claim 26, further comprising the step of downloading the connection policy from a central administration.

33. The method of claim 26, further comprising the steps of displaying an access control user interface, receiving input from a user of the end system, using the input to define the rules of the connection policy.